REMARKS

Claims 29–32, 34–36, 38–48, and 50–54 are pending in this application. The amendments broaden some aspects of the previously presented claims.

I. CLAIM REJECTIONS BASED ON 35 U.S.C. § 103

Claims 29-36 and 38-54 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 7,036,020 to Thibadeau ("*Thibadeau*") and further in view of PCT Publication No. WO 03/003242 to Hearn et al. ("*Hearn*"). Applicants traverse the rejection. Reconsideration is respectfully requested.

INDEPENDENT CLAIM 29

Claim 29 recites among other elements:

> a security partition formed in the storage device, the **operating system of the computer** being **stored in the security partition**; and
> a security device comprising a hardware processor or controller for intercepting communications and **selectively blocking access to operating system data** between the host CPU and the security partition;
> wherein the security device is deployed along the chain of components that connect the host CPU to the storage device;
> wherein the security device's processor or controller is distinct from the host CPU; and
> wherein **during operation of the operating system** the security device is arranged to: **intercept** requests to write **changes to operating system files in the security partition**; in response to the requests, **instead of write the changes to the operating system files in the security partition as targeted by the requests, write the changes to a location different than the security partition**; and cause normal operation of the operating system to continue **without writing the changes to the operating system files in the security partition**.

The cited references fail to teach or suggest at least the above bolded elements of Claim 29.

(1) The references do not "selectively block[] access to operating system data"

The security device of Claim 29 selectively blocks access to operating system data. While the Final Office Action alleges that *Thibadeau* describes such a security device, the Advisory Action instead asserts that the feature is described in one of the other cited references; thus, the Advisory Action appears to confirm that the Office now agrees with Applicants that *Thibadeau* does not describe selectively blocking access to operating system data, as stated in Applicants' previous reply.

The Advisory Action asserts that *Hearn* describes a security device that "selectively block[s] access to operating system data" at page 16, lines 7–17, which reads:

> The security device CPU 37 operates according to a prescribed application program stored in the flash ROM 41 and which is loaded into the RAM 39 on start up and becomes the operating system for the security device. The CPU 37 communicates with the bus control and interface logic 43, which is interposed in line with the ATA cable 33 to intercept communications between the host CPU 13 and the storage media 21. The secure media interface 45 is interposed between the bus control and interface logic 43 and the custom interface 49 to facilitate communications between the host CPU 13 and the secure storage media 47 under the control of the CPU 37.

The Advisory Action is mistaken. The above-quoted passage merely describes that, as part of the startup routine for a security device that selectively blocks files, the security device loads an "operating system for the security device" (e.g. device firmware) from the flash ROM 41 of the security device into the RAM 39 of the security device. Claim 1, by contrast, recites an entirely different "operating system of the computer." One of ordinary skill in the art would

have clearly understood that the recited **operating system of the computer** is separate and different from the **operating system of the security device** described in the above quoted passage of *Hearn*.

In fact, both *Hearn* and Applicants' Specification clearly differentiate between the operating system of a computer and the operating system of a security device. For example, *Hearn* at page 12, lines 3–7 explains "said selective blocking [performed by the security device] occurs during initialisation of the computer and includes intercepting all said data access during the start up sequence immediately after said initialisation and before loading of the operating system of the computer." The loading of the operating system of the security device to initialize the security device would occur before the operating system of the computer is ever loaded. Thus, the loading of the operating system of the security device could not have suggested anything about how the security device interacts with the operating system of the computer.

Moreover, even if the operating system loaded into RAM 39 of the security device could be considered "the operating system of the computer," which it cannot, the operating system loaded into RAM 39 of the security device is clearly loaded "**from ROM 41 of the security device**." As such, the operating system loaded into RAM 39 is not **"operating system data [in] the security partition"** as recited in Claim 29. Nor is there any evidence that the operating system data in RAM 39 is ever accessed or even requested by the host CPU of the computer, as recited in Claim 29.

Furthermore, the Claim 29 recites "selectively blocking access to operating system data." The loading of operating system data into RAM 39 of the security device, even if that operating system data had been "of the computer" and from "the security partition," does not imply that operating system data is ever "blocked," much less "selectively." Clearly, then, the relied upon

passages of *Hearn* do not teach or suggest "selectively blocking access to operating system data between the host CPU and the security partition" as recited in Claim 29.

(2) The references do not describe "instead of writ[ing] the changes to the operating system files in the security partition . . ., writ[ing] the changes to a location different than the security partition."

The Advisory Action alleged, without explanation, that page 15, lines 2 to 8, and page 5, line 24 to page 17, line 8 of *Hearn* describe "divert[ing] . . . operating system files to a location different than the security partition." Applicants disagree, for at least reasons similar to those already stated above. However, Claim 29 now recites that the security device, "**instead of writ[ing]** the changes to the operating system files **in the security partition** as targeted by the requests, **write[s]** the changes **to a location different than the security partition**." *Hearn* clearly recites no such feature.

Hearn describes that a security device selectively blocks access to certain types of data in a security partition. However, the security device described in *Hearn* does not respond to requests to write to a security partition by writing to another location instead of the security partition. Because the security device of *Hearn* is only capable of blocking access to data, the security device would have been unable to block changes to operating system files in a security partition without causing operating system errors. By contrast, because the security device of Claim 29 diverts write operations to a different location, the security device of Claim 29 is able to "cause normal operation of the operating system to continue without writing the changes to the operating system files in the security partition."

For at least the foregoing reasons, the combination of *Thibadeau* and *Hearn* fails to provide the complete subject matter recited in independent Claim 29. Therefore, the

combination of *Thibadeau* and *Hearn* would not have rendered Claim 29 obvious under 35 U.S.C. § 103. Reconsideration is respectfully requested.

REMAINING CLAIMS

Each of the remaining claims recites or depends from a claim that recites at least one of the above-discussed features. As discussed above, the combination of *Thibadeau* and *Hearn* fails to teach or suggest the above-discussed features. The remaining cited references also do not appear to teach, and are not alleged to teach, the above-discussed features. Consequently, the combination of *Thibadeau* and *Hearn* fails to teach or suggest the complete subject matter of the remaining claims.

Moreover, the remaining pending claims include additional elements that the cited references also do not teach or suggest. However, to expedite prosecution, arguments concerning these additional elements are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and these additional novel elements.

II. CONCLUSION

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact Applicants' representative by telephone relating to any issue that would advance examination.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, the fee for the petition for extension of time fee and other applicable fees is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: August 17, 2011

/KarlTRees#58983/
Karl T. Rees, Reg. No. 58,983

2055 Gateway Place, Suite 550
San Jose, CA 95110
(408) 414-1233
Facsimile: (408) 414-1076